UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,557	07/27/2001	Marc Girault	211526US2PCT	7668

22850 7590 01/31/2005

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 01/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/889,557	GIRAULT ET AL.	
	Examiner	Art Unit	
	Venkatanarayanan Perungavoor	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8,9 and 12-14* is/are rejected.

7)☒ Claim(s) *10 and 11* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specifications

1. On Page 1, Line 17, the Applicant mentions " recognised" and the examiner believes the applicant meant "recognized". Appropriate changes required.

2. On Page 2, Line 27, the Applicant is missing quotation marks after "...memory"

3. On Page 5, Line 9, the Applicant mentions "optimisation" and the examiner believes the applicant meant "optimization". Appropriate changes required.

Claim Rejections – 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 8-14 are rejected under U.S.C. 101 because the subject matter disclosed is limited to a mathematical algorithm and also the subject matter lacks technological implementation.

Claim Rejections – 35 USC § 102

6.The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7.Claim 8-9,13-14 rejected under 35 U.S.C. 102(b) as being anticipated by EP 0325 238 A2 to Shamir, Adi .

8. Regarding Claim 8, The "authentication process involving a first entity, which possesses a public key v and a secret key s, these keys being related by an operation modulo n, where n is an integer, the modulus n being specific to the first entity and a second entity, which knows the public key v, these entities being provided with means to exchange zero-knowledge information and carry out cryptographic calculations on this information, some calculations being carried out modulo n, the process being characterized in that the modulo n operation is of the kind $v=s^{-t} \pmod n$, t being a parameter" is met by Shamir see Abstract & Page 4 Line 33-49.

9. Regarding Claim 9, The "first entity selects at least one integer at random ranging between 1 and n-1 and calculates at least one parameter x equal to $r^t \pmod n$, then at least one number c that is at least one function of the at least one of a parameter and a message, and sends the at least one number c to the second entity; the second entity receives the c, selects one number e at random and sends this question to the first entity; the first entity receives the question e, carries out at least one calculation using the at least one number e and the secret key s, the result of the at least one calculation

yielding at least one answer y and sends the at least one answer y to the second entity. The second entity receives the answer y, carries out one calculation using the public key v and the modulus n, and checks with a modulo n calculation that the result is coherent with the received at least one number c" is met by Shamir see Page 2 Line 44 - Page 3 Line 41.

10. Regarding Claim 13, The "a message signature process configured for a signatory provided with a public key v and a secret key s, the public and private keys being related by a modulo n calculation, where n is an integer, which is specific to the signatory, the process utilizing means configured to calculate at least one number c that is a function of a message M to be signed, configured to calculate at least one number y that is a function of the secret key s, and configured to transmit the numbers y and c that are the signature of the message and the message M, wherein the modulo n operation is $v=s^{-t}(\text{mod } n)$, t being a parameter" is met by Shamir see Abstract & Page 4 Line 33-49 & Page 2 Line 44 - Page 3 Line 41.

11. Regarding Claim 14, The "the signatory selects an integer r at random between 1 and n-1, calculates a parameter x equal to r^t (mod n), calculates at least one number e that is a function of parameter x and the message M to be signed, calculates the at least one number y using its secret key s, said at least one number y being a function of

numbers r and e, and transmits the numbers c and y as the signature" is met by Shamir see Page 2 Line 44 - Page 3 Line 41.

Claim Rejections- 35 USC §103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claim 12 rejected under 35 U.S.C. 103(a) as being unpatentable over EP 0325 238 A2 to Shamir in view of NPL[1] to Schneier.

14. Regarding Claim 12, Shamir discloses the n being an product of two prime numbers see Page 4 Line 14-22 and further discloses the use of quadratic residue for modulo n operation. However, Schneier discloses the use of Chinese remainder method see Page 249-250. It would be obvious to one having ordinary skill in the art at the time of the invention to modify Shamir's invention of quadratic residue modulo method to Chinese remainder modulo method in order to have only two uniquely numbers.

Allowable Subject Matter

[1] See Attached Non-Patent Literature(Applied Cryptography- Protocols, Algorithms and Source Code in C by Bruce Schneier 2rd Edition) Pages 249-250.

15. Regarding Claim 10 and Claim 11 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

17. The following patents are cited to further show the state of art in general:

U.S. Patent No. 5218637 to Angebaud et al.

PCT Publication Number WO 89/11706 to Austin et al.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkatanarayanan Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Venkatanarayanan Perungavoor
Examiner
Art Unit 2132

VP
1/11/05

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100